(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 102 47 794 A1** 2004.04.22

(12) # Offenlegungsschrift

(21) Aktenzeichen: **102 47 794.9**
(22) Anmeldetag: **14.10.2002**
(43) Offenlegungstag: **22.04.2004**

(51) Int Cl.[7]: **G06K 19/07**

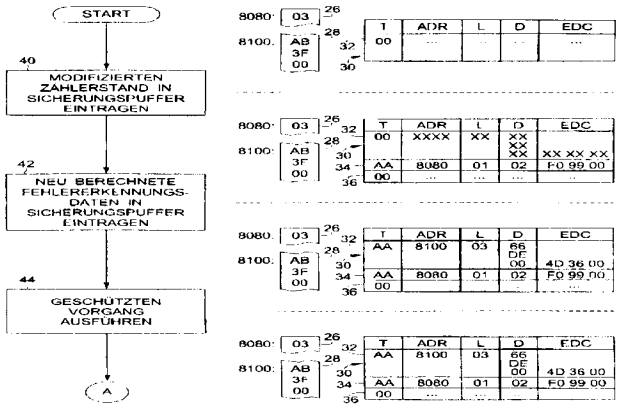
(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Schmalz, Frank, 82008 Unterhaching, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verwalten eines Fehlversuchszählers in einem tragbaren Datenträger**

(57) Zusammenfassung: Bei einem Verfahren zum Verwalten eines Fehlversuchszählers (26) in einem nicht-flüchtigen Speicher eines einen Sicherungspuffer aufweisenden, tragbaren Datenträgers wird ein Eintrag (34) in den Sicherungspuffer (30) des Datenträgers eingeschrieben, wobei der Eintrag (34) einen Wert enthält, der einem neuen Stand des Fehlversuchszählers (26) nach einem angenommenen Fehlversuch entspricht, so daß dieser Wert bei einem zumindest im Zusammenhang mit einem Neustart des Datenträgers ausgelösten Wiederherstellungsvorgang in den Fehlversuchszähler (26) eingeschrieben wird. Ein tragbarer Datenträger und ein Computerprogrammprodukt weisen entsprechende Merkmale auf. Die Erfindung stellt eine Technik zum Verwalten eines Fehlversuchszählers in einem tragbaren Datenträger bereit, die ohne Sicherheitseinbußen nur einen geringen Zeitbedarf im Gutfall aufweist und nur eine geringe Belastung des nicht-flüchtigen Speichers des Datenträgers verursacht.



Beschreibung

[0001] Die Erfindung betrifft allgemein tragbare Datenträger wie z.B. Chipkarten (smart cards) und Chipmodule in unterschiedlichen Bauformen. Spezieller betrifft die Erfindung die Verwaltung von Fehlversuchszählern in solchen Datenträgern.

[0002] Fehlversuchszähler dienen allgemein der Überwachung der Anzahl von Fehlversuchen beim Ausführen eines geschützten Vorgangs. Bei Überschreitung einer vorgegebenen Fehlversuchs-Maximalzahl werden einzelne oder alle Funktionen des Datenträgers gesperrt. Dies ist besonders für sicherheitskritische Anwendungen wichtig, weil jeder Fehlversuch potentiell auf einen Angriff hinweisen kann. Durch Fehlversuchszähler wird in der Regel die Eingabe von geheimen Kennwerten wie z.B. Schlüsseln oder persönlichen Geheimzahlen (PINs – personal identrfication numbers) abgesichert, um einen Angreifer daran zu hindern, den geheimen Kennwert durch Ausprobieren einer Vielzahl von Eingaben zufällig zu erraten. In diesem Zusammenhang wird der Fehlversuchszähler oft auch als Fehlbedienungszähler (FBZ) bezeichnet.

Stand der Technik

[0003] Auf Seite 504 des Buches "Handbuch der Chipkarten" von W. Rankl und W. Effing, Carl Hanser Verlag, 3. Auflage, 1999, ist es als Angriffsmöglichkeit beschrieben, die Spannungsversorgung der Chipkarte nach Erkennung eines Fehlversuchs, aber bevor der Stand des Fehlversuchszählers verändert wird, abzuschalten. Wenn dies gelingt, kann die durch den Fehlversuchszähler bewirkte Beschränkung der Versuchsanzahl ausgehebelt werden. Es wird daher vorgeschlagen, den Stand des Fehlversuchszählers vor der Ausführung des geschützten Vorgangs zunächst immer zu erhöhen, so daß bei einer Spannungsunterbrechung ab diesem Zeitpunkt stets ein Fehlversuch registriert wird. Erst nach einer erfolgreichen Ausführung des geschützten Vorgangs wird der Zählerstand wieder auf den ursprünglichen Wert oder auf einen vorgegebenen Initialwert zurückgesetzt.

[0004] Dieses Verfahren hat allerdings den Nachteil, daß der Zählerstand im Gutfall zwei Mal verändert werden muß. Dies stellt einen erheblichen Zeitaufwand und eine erhebliche Belastung des nicht-flüchtigen Speichers, in dem der Fehlversuchszähler angelegt ist, dar. Bei typischen Implementierungen müssen nämlich bei jeder Veränderung des Fehlversuchszählers auch noch Fehlererkennungsdaten zur Absicherung gegen Speicherfehler geschrieben werden. Diese Schreibvorgänge müssen überdies als atomare Transaktion ausgeführt werden, so daß weiterer Aufwand zur Verwaltung eines Sicherungspuffers erforderlich ist.

[0005] Aus dem US-Patent 4,922,456 ist ein Verfahren zum Schreiben von Daten in einen nicht-flüchtigen Speicher bekannt, bei dem die Daten und deren Zieladresse im Speicher zunächst in einen Puffer geschrieben werden. Erst nach Abschluß dieses Schreibvorgangs werden die Daten in den nicht-flüchtigen Speicher übertragen. Wird der Übertragungsvorgang durch eine Spannungsunterbrechung gestört, so wird er bei der nächsten Inbetriebnahme des Systems nachgeholt.

[0006] Das deutsche Patent DE 196 00 081 C2 offenbart ein Verfahren zur Sicherung der Integrität von Daten bei einer Kommunikation unter Beteiligung einer Datenträgerkarte, bei dem eine Kopie eines zu verändernden Datenbestandes in einem Schattenspeicher angelegt wird und die einzelnen Schreibvorgänge nur an dem Datenbestand oder nur an dessen Kopie ausgeführt werden.

Aufgabenstellung

[0007] Die Erfindung hat die Aufgabe, die genannten Probleme zumindest zum Teil zu lösen. Insbesondere soll durch die Erfindung eine Technik zum Verwalten eines Fehlversuchszählers in einem tragbaren Datenträger bereitgestellt werden, die ohne Sicherheitseinbußen einen möglichst geringen Zeitbedarf im Gutfall aufweist und eine möglichst geringe Belastung des nichtflüchtigen Speichers des Datenträgers verursacht.

[0008] Erfindungsgemäß wird diese Aufgabe ganz oder zum Teil gelöst durch ein Verfahren mit den Merkmalen von Anspruch 1, einen Datenträger gemäß Anspruch 11 und ein Computerprogrammprodukt gemäß Anspruch 12. Die abhängigen Ansprüche definieren bevorzugte Ausgestaltungen der Erfindung. Die Aufzählungsreihenfolge der Schritte in den Verfahrensansprüchen soll nicht als Einschränkung des Schutzbereichs verstanden werden. Es sind vielmehr Ausgestaltungen der Erfindung vorgesehen, bei denen diese Verfahrensschritte in anderer Reihenfolge oder ganz oder teilweise parallel oder ganz oder teilweise ineinander verzahnt (interleaved ausgeführt werden.

[0009] Die Erfindung geht von der Grundidee aus, zum Zwecke der Absicherung des Fehlversuchszählers gegen eine Unterbrechung der Versorgungsspannung des Datenträgers einen Sicherungspuffer des Datenträgers einzusetzen. Der Datenträger ist so eingerichtet, daß bei einem Wiederherstellungsvorgang Daten aus aktiven Einträgen des Sicherungspuffers in den Speicher des Datenträgers übertragen werden; ein solcher Wiederherstellungsvorgang wird zumindest im Zusammenhang mit einem Neustart des Datenträgers, z.B. nach einem Ausfall der Versorgungsspannung, ausgelöst. Erfindungsgemäß ist nun vorgesehen, in den Sicherungspuffer einen Eintrag einzuschreiben, der einen Wert enthält, welcher einem neuen Stand des Fehlversuchszählers nach einem angenommenen Fehlversuch entspricht.

[0010] Die erfindungsgemäße Nutzung des Sicherungspuffers bewirkt, daß auch bei einem Ausfall der

Versorgungsspannung ein neuer Wert des Fehlversuchszählers, der den Fehlversuch wiedergibt, in den Fehlversuchszähler eingeschrieben wird. Angriffe wie die eingangs mit Hinweis auf das Buch von Rankl und Effing genannten werden damit zuverlässig vermieden. Im Gutfall, also wenn der geschützte Vorgang erfolgreich ausgeführt worden ist, braucht der Fehlversuchszähler nicht verändert zu werden, sofern er nicht auf einen vorgegebenen Initialwert gesetzt werden soll. Insgesamt ergibt sich somit im Gutfall ein erheblich geringerer Zeitaufwand und eine erheblich geringere Belastung des nicht-flüchtigen Speichers durch Schreibvorgänge.

[0011] Erfindungsgemäß wird durch den Fehlversuchszähler die Anzahl von Fehlversuchen bei der Ausführung eines geschützten Vorgangs überwacht. Der geschützte Vorgang kann z.B. ein als "Schlüsseloperation" bezeichneter Vergleich eines internen geheimen Kennwerts mit einem von außen in den Datenträger eingegebenen Wert sein. Ist dieser Vergleich erfolgreich, so wird vorzugsweise der Stand des Fehlversuchszählers nicht verändert oder – falls erforderlich – auf einen Initialwert zurückgesetzt. Ferner wird dann in bevorzugten Ausführungsformen der Inhalt des Sicherungspuffers verworfen.

[0012] Bei einer fehlgeschlagenen Ausführung des geschützten Vorgangs ist dagegen vorzugsweise eine Veränderung des Standes des Fehlversuchszählers vorgesehen, die in unterschiedlichen Ausgestaltungen entweder eine Dekrementierung oder eine Inkrementierung sein kann. Um diese Veränderung zu bewirken, kann in manchen Ausführungsformen der Erfindung der Wiederherstellungsvorgang auch ohne einen Neustart des Datenträgers ausgeführt werden.

[0013] Vorzugsweise ist der Sicherungspuffer Teil eines Transaktionsmechanismus, der vom Betriebssystem des Datenträgers auch zu anderen Zwecken – also nicht nur zur Verwaltung des Fehlversuchszählers – bereitgestellt wird. Dieser Transaktionsmechanismus kann so ausgestaltet sein, daß der Sicherungspuffer normalerweise entweder eine Kopie des ursprünglichen Speicherinhalts vor Beginn der Transaktion oder ein Duplikat der einzuschreibenden Daten enthält. In beiden Fällen wird jedoch bei der erfindungsgemäßen Nutzung des Transaktionsmechanismus der veränderte Stand des Fehlversuchszählers in den Sicherungspuffer eingetragen, und der Eintrag im Sicherungspuffer wird derart markiert, daß die in diesem Eintrag enthaltenen Daten bei einem Wiederherstellungsvorgang in den Speicher des Datenträgers eingeschrieben werden.

[0014] Vorzugsweise ist die Verwendung von Fehlererkennungsdaten zumindest für kritische Speicherbereiche des Datenträgers vorgesehen. Diese kritischen Speicherbereiche können insbesondere den Fehlversuchszähler und/oder den Sicherungspuffer enthalten. Entsprechend können sich die Einträge im Sicherungspuffer auch auf die zum neuen Stand des Fehlversuchszählers gehörigen Fehlererkennungsdaten beziehen, und die Einträge können ihrerseits Fehlererkennungsdaten enthalten.

[0015] Das erfindungsgemäße Computerprogrammprodukt weist Programmbefehle auf, um das erfindungsgemäße Verfahren zu implementieren. Ein derartiges Computerprogrammprodukt kann ein körperliches Medium sein, beispielsweise ein Halbleiterspeicher oder eine Diskette oder eine CD-ROM, auf dem ein Programm zur Ausführung des erfindungsgemäßen Verfahrens gespeichert ist. Das Computerprogrammprodukt kann jedoch auch ein nichtkörperliches Medium sein, beispielsweise ein über ein Computernetzwerk übermitteltes Signal. Das Computerprogrammprodukt kann insbesondere ein Betriebssystem oder Teil eines Betriebssystems für tragbare Datenträger sein, das im Zusammenhang mit der Herstellung und/oder Initialisierung und/oder Personalisierung der Datenträger in diese eingebracht wird.

[0016] Der tragbare Datenträger und das Computerprogrammprodukt weisen in bevorzugten Weiterbildungen Merkmale auf, die den oben erwähnten und/oder den in den abhängigen Verfahrensansprüchen genannten Merkmalen entsprechen.

[0017] Weitere Merkmale, Aufgaben und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung eines Ausführungsbeispiels und mehrerer Ausführungsalternativen. Es wird auf die schematischen Zeichnungen verwiesen, in denen zeigen:

[0018] **Fig.** 1 ein Blockdiagramm eines tragbaren Datenträgers mit Komponenten, die für das hier beschriebene Ausführungsbeispiel relevant sind, und

[0019] **Fig.** 2 ein Ablaufdiagramm des Verfahrens im hier beschriebenen Ausführungsbeispiel bis zur Ausführung des geschützten Vorgangs,

[0020] **Fig.** 3 ein an **Fig.** 2 anknüpfendes Ablaufdiagramm bei einer erfolgreichen Ausführung des geschützten Vorgangs, und

[0021] **Fig.** 4 ein Ablaufdiagramm eines Wiederherstellungsvorgangs, bei dem der Fehlversuchszähler auf einen neuen Zählerstand gesetzt wird.

Ausführungsbeispiel

[0022] In **Fig.** 1 ist ein tragbarer Datenträger **10** gezeigt, der beispielsweise als Chipkarte oder Chipmodul ausgebildet ist. In an sich bekannter Weise weist der Datenträger **10** einen Halbleiterchip auf, auf dem ein Prozessorkern **12**, ein Speicher **14** und eine Schnittstelle **16** zur drahtgebundenen oder drahtlosen Kommunikation ausgebildet sind. Der Speicher **14** weist mehrere unterschiedliche Bereiche auf, nämlich im vorliegenden Ausführungsbeispiel einen als maskenprogrammiertes ROM (read only memory) ausgestalteten Festwertspeicher **18**, einen als RAM (random access memory) ausgestalteten, flüchtigen Arbeitsspeicher **20** und einen als EEPROM (electrically erasable programmable read only memory) ausgestalteten, nicht-flüchtigen, beschreibbaren Speicher **22**.

[0023] In an sich bekannter Weise enthält der Festwertspeicher **18** wesentliche Teile des Betriebssystems des Datenträgers **10** und der von diesem Betriebssystem ausgeführten Programme. Im nicht-flüchtigen, beschreibbaren Speicher **22** befindet sich ein Dateisystem **24**, das im hier beschriebenen Ausführungsbeispiel der Norm ISO 7816 entspricht und das eine Wurzel sowie Verzeichnisse und Dateien in mehreren Hierarchieebenen aufweist. Insbesondere enthält das Dateisystem **24** eine ein Byte große Datei "EF_KEYD", die einen Fehlversuchszähler **26** bildet. Dem Dateisystem **24** sind Fehlererkennungsdaten **28** zugeordnet, die in an sich bekannter Weise verwendet werden, um dauerhafte oder temporäre Fehler im nicht-flüchtigen Speicher **22** zu erkennen. Zumindest der Fehlversuchszähler **26** ist über diese Fehlererkennungsdaten **28**, die Prüfsummen einzelner Speicherzellen oder Speicherbereiche enthalten, abgesichert.

[0024] Das Betriebssystem des Datenträgers **10** stellt einen für diverse Aufgaben vorgesehenen Mechanismus zur Verwaltung von Transaktionen bereit. Allgemein definiert eine Transaktion eine unteilbare Sequenz von Schreibvorgängen. Die Transaktionsverwaltung stellt sicher, daß von diesen Schreibvorgängen entweder alle oder keiner ausgeführt wird. Zu diesem Zweck nutzt die Transaktionsverwaltung einen im nicht-flüchtigen Speicher **22** befindlichen Sicherungspuffer **30**, in dem – je nach Ausgestaltung des Transaktionsmechanismus – bis zum Abschluß der Transaktion entweder die ursprünglich im Speicher **22** vorhandenen Daten oder die neu in den Speicher **22** einzuschreibenden Daten enthalten sind. Welche dieser beiden Varianten vorliegt, spielt für die hier gegebene Beschreibung so gut wie keine Rolle, da bei der erfindungsgemäßen Verwendung des Transaktionsmechanismus stets Daten, die einem neuen Zählerstand des Fehlversuchszählers **26** nach einem potentiellen Fehlversuch entsprechen, in den Sicherungspuffer **30** eingeschrieben werden.

[0025] Im vorliegenden Ausführungsbeispiel weist der Sicherungspuffer **30** Einträge mit jeweils mehreren Datenfeldern auf, nämlich einem Kennzeichen T (tag), einer Adresse ADR, die die Startadresse der im Fehlerfall zu schreibenden Daten angibt, einer Längenangabe L der Daten und den eigentlichen Daten D. Ferner ist in jedem Eintrag im Sicherungspuffer **30** ein Feld für Fehlererkennungsdaten EDC (error detection code) enthalten, um die Fehlerfreiheit des Eintrags überprüfen zu können.

[0026] Es ist eine wichtige Eigenschaft des Transaktionsmechanismus, daß die oben erwähnte Atomizität vom Transaktionen auch dann sichergestellt ist, wenn die Versorgungsspannung des Datenträgers **10** oder die Kommunikationsverbindung zwischen dem Datenträger **10** und einem Terminal während der Ausführung einer Transaktion unerwartet unterbrochen wird (sogenanntes tear-Ereignis). Um dies zu gewährleisten, wird beim Neustart des Datenträgers **10** nach dem tear-Ereignis der Sicherungspuffer **30** auf aktive Einträge untersucht, um entweder den ursprünglichen Speicherzustand vor Beginn der Transaktion wieder herzustellen oder alle noch nicht ausgeführten Schreibvorgänge der Transaktion nachzuholen.

[0027] In dem hier beschriebenen Datenträger **10** ist die Transaktionsverwaltung derart erweitert, daß sie in effizienter Weise auch zur Verwaltung von Fehlversuchszählern – hier beispielsweise des Fehlversuchszählers **26** – eingesetzt werden kann. Dazu stellt die Transaktionsverwaltung eine zusätzliche Funktion bereit, die eine mögliche Änderung des Standes des Fehlversuchszählers **26**, welche einen Fehlversuch anzeigt, in dem Sicherungspuffer **30** vormerkt. Diese Vormerkung erfolgt stets so, daß der im Sicherungspuffer **30** eingetragene, neue Zählerstand bei einem Unterbrechungsfall und dem darauffolgenden Neustart des Datenträgers **10** in den Fehlversuchszähler **26** geschrieben wird. Bei Ausgestaltungen der Transaktionsverwaltung, die im Sicherungspuffer **30** normalerweise die zu schreibenden Daten ablegen, wird die durch den Vormerkungsvorgang begonnene Transaktion daher als vollständig gekennzeichnet. In Ausgestaltungen, bei denen der Sicherungspuffer **30** normalerweise die ursprünglichen Daten enthält, wird dagegen die Transaktion bewußt noch als offen markiert, damit während des Neustarts die vermeintlich ursprünglichen Daten – in Wirklichkeit aber der modifizierte Zählerstand – in den Fehlversuchszähler **26** eingeschrieben wird.

[0028] **Fig.** 2 zeigt einen beispielhaften Ablauf dieser Vormerkung mit der darauffolgenden Ausführung des geschützten Vorgangs. Der linke Teil von **Fig.** 2 stellt die einzelnen Verfahrensschritte dar, während im rechten Teil der jeweilige Inhalt einiger Bereiche des nicht-flüchtigen Speichers **22** angegeben ist. Diese Bereiche sind erstens der Fehlversuchszähler **26**, der sich im vorliegenden Beispiel an der Speicheradresse **8080** befindet, zweitens drei Byte der Fehlererkennungsdaten **28** mit der Startadresse **8100**, welche zur Absicherung des Fehlversuchszählers **26** dienen, und drittens der Sicherungspuffer **30**. Alle Speicherwerte und Speicheradressen sind im vorliegenden Text und in den Zeichnungsfiguren stets in hexadezimaler Schreibweise angegeben.

[0029] Im anfänglichen Speicherzustand von **Fig.** 2 weist der Fehlversuchszähler **26** den Zählerstand **03** auf, wodurch angezeigt wird, dal3 bis zu einer Sperrung des Datenträgers **10** noch drei Fehlversuche zulässig sind. Bei jedem Fehlversuch wird im vorliegenden Ausführungsbeispiel der Zählerstand dekrementiert. Es sind jedoch auch Ausgestaltungen vorgesehen, bei denen der Fehlversuchszähler **26** bei jedem Fehlversuch inkrementiert wird. Die Fehlererkennungsdaten **28** ab der Speicheradresse **8100**, die dem Fehlversuchszähler **26** zugeordnet sind, lauten beispielsweise AB 3F 00. Im Sicherungspuffer **30** ist ein einziger Eintrag **32** enthalten, der den Wert 00 als Kennzeichen T aufweist. Dieser Wert kennzeichnet einen inaktiven Eintrag und gleichzeitig das Pufferen-

de. Der Sicherungspuffer **30** ist damit leer.

[0030] Als erster Schritt 40 des bereits erwähnten Vormerkungsvorgangs wird in den Sicherungspuffer **30** ein neuer Wert für den Fehlversuchszähler **26** eingetragen, der einem neuen Zählerstand bei einem angenommenen Fehlversuch entspricht. Im vorliegenden Beispiel ist dies der Wert 02. Ferner wird ein entsprechender Eintrag **34** im Sicherungspuffer **30** erstellt, der den Wert AA als Kennzeichen für eine lokale Transaktion, die Adreßangabe **8080** als Speicheradresse des Fehlversuchszählers **26**, die Bytelänge **01**, den Datenwert **02** als neuen Stand des Fehlversuchszählers **26** und die den Eintrag **34** absichernden Fehlererkennungsdaten F0 99 00 aufweist. Ein weiterer Eintrag **36** mit einem Kennzeichen **00** bezeichnet das Pufferende.

[0031] Im vorliegenden Ausführungsbeispiel wird der Eintrag **34** als zweiter Eintrag mit einem Versatz (offset) von zehn Byte gegenüber dem Anfang des Sicherungspuffers **30** in diesen eingetragen. Mit anderen Worten wird der Sicherungspuffer **30** von "hinten nach vorne" – also in entgegengesetzter Richtung zur Auswertungsreihenfolge bei einem möglichen Wiederherstellungsvorgang bei einem Neustart des Datenträgers **10** – gefüllt. Wenn zum jetzigen Zeitpunkt ein Spannungsausfall oder ein tear-Ereignis erfolgen würde, würde bei dem Wiederherstellungsvorgang zunächst der Eintrag **32** mit dem Kennzeichen **00** ausgewertet werden. Da der Kennzeichnungswert **00** das Ende des Sicherungspuffers **30** markiert, würde dann die Auswertung ohne einen Schreibvorgang in den Speicher **22** beendet werden. Auf diese Weise wird ein inkonsistenter Zustand zwischen dem Fehlversuchszähler **26** und den entsprechenden Fehlererkennungsdaten **28** vermieden, der auftreten könnte, wenn in Schritt 40 zunächst der erste Eintrag **32** geschrieben werden würde. Im Ergebnis werden daher der vorliegende Schritt 40 und der folgende Schritt 42 wie eine atomare Transaktion ausgeführt.

[0032] Wie bereits angedeutet, werden in Schritt 42 neu berechnete Fehlererkennungsdaten, die an den vorgemerkten Zählerstand **02** des Fehlversuchszählers **26** angepaßt sind, in den Sicherungspuffer **30** geschrieben. Dieser Eintrag bildet einen neuen ersten Eintrag **32**. Die Byteanzahl des neuen ersten Eintrags **32** entspricht dem im vorhergehenden Schritt 40 gewählten Versatz für den zweiten Eintrag **34**, also im vorliegenden Beispiel zehn Byte. Wie in

[0033] **Fig.** 2 dargestellt, weist der neue erste Eintrag **32** das Kennzeichen AA mit der Bedeutung einer lokalen Transaktion auf. Der Eintrag **32** enthält ferner die Zieladresse **8100** für die einzuschreibenden Daten, die Datenlänge **03** und die drei Datenbyte **66** DE 00 als Fehlererkennungsdaten für den Zählerstand **02**. Außerdem enthält der neue erste Eintrag **32** eigene Fehlererkennungsdaten mit den beispielhaften Werten 4D 36 00.

[0034] Der Vormerkungsvorgang ist damit beendet. Im nun folgenden Schritt 44 wird der geschützte Vorgang ausgeführt. Typischerweise ist dieser geschützte Vorgang ein als Schlüsseloperation bezeichneter Vergleich einer internen Geheimzahl oder eines internen Schlüssels mit einem externen Wert, den der Datenträger über die Schnittstelle **16** erhalten hat. Der Inhalt der in **Fig.** 2 dargestellten Speicherbereiche wird durch diesen Vorgang nicht verändert.

[0035] Im Gutfall, also wenn sich bei dem Vergleich eine Übereinstimmung ergeben hat, wird das Verfahren gemäß **Fig.** 3 fortgesetzt. Hierbei werden in Schritt 46 die im Sicherungspuffer **30** enthaltenen Einträge **32** und **34**, die lediglich einen neuen Stand des Fehlversuchszählers **26** für einen möglichen Schlechtfall enthalten, deaktiviert. Hierzu reicht es aus, das Kennzeichen T des ersten Eintrags **32** auf den Wert 00 zu setzen, der das Ende des Sicherungspuffers **30** angibt. Der weitere Inhalt des Sicherungspuffers **30** braucht nicht überschrieben zu werden.

[0036] Insgesamt sind somit im Gutfall 20 Byte in den nicht-flüchtigen Speicher **22** geschrieben worden, nämlich neun Byte bei Schritt 40, zehn Byte bei Schritt 42 und ein Byte bei Schritt 46.

[0037] Im hier beschriebenen Ausführungsbeispiel wird der Stand des Fehlversuchszählers **26** im Gutfall nicht verändert. Es sind jedoch auch Ausgestaltungen vorgesehen, bei denen der Fehlversuchszähler **26** im Gutfall stets auf einen vorgegebenen Initialwert – beispielsweise den Wert 03 – gesetzt wird. Dies braucht natürlich nur dann zu geschehen, wenn der aktuelle Zählerstand von diesem Initialwert abweicht. Bei jeder Veränderung des Zählerstands sind auch die zugehörigen Fehlererkennungsdaten **28** entsprechend anzupassen.

[0038] Falls bei der Ausführung des geschützten Vorgangs, also z.B. der Schlüsseloperation, in Schritt 44 eine Unterbrechung der Stromversorgung oder ein tear-Ereignis erfolgt, führt der Datenträger **10** auf an sich bekannte Weise beim nächsten Neustart – genauer gesagt, als Reaktion auf das erste eingehende Kommando – eine Prüfung auf noch zu bearbeitende Transaktionen durch. Solche Transaktionen werden durch aktive Einträge im Sicherungspuffer **30** angezeigt. Im vorliegenden Beispiel liegen zwei aktive Einträge **32**, **34** vor, welche dann in einem Wiederherstellungsvorgang der Reihe nach abgearbeitet werden.

[0039] **Fig.** 4 zeigt den Ablauf dieses Wiederherstellungsvorgangs. Ausgehend von dem Speicherzustand während der Ausführung des geschützten Vorgangs wird zunächst – in Schritt 48 – der erste Eintrag **32** im Sicherungspuffer **30** verarbeitet. Hierbei werden die Fehlererkennungsdaten **66** DE 00, die auf den dekrementierten Stand **02** des Fehlversuchszählers **26** zugeschnitten sind, mit der Startadresse **8100** in den Speicher **22** geschrieben. Bei der Verarbeitung des zweiten Eintrags **34** in Schritt 50 wird dann der neue Zählerstand **02** in den Fehlversuchszähler **26**, also an die Speicheradresse **8080**, eingetragen. Der konsistente Zustand zwischen dem Stand des Fehlversuchszählers **26** und den zugeordneten Fehlerer-

kennungsdaten **28** ist damit wieder hergestellt.

[0040] In einem abschließenden Schritt 52 werden die Einträge **32**, **34** im Sicherungspuffer **30** deaktiviert, indem der Kennzeichnungswert **00** in das tag-Feld des ersten Eintrags **32** geschrieben wird. Ebenso wie in dem in **Fig.** 3 dargestellten Gutfall ist kein weiteres Überschreiben des Inhalts des Sicherungspuffers **30** erforderlich.

[0041] Bislang wurden der Gutfall sowie der Fall einer Unterbrechung während der Ausführung des geschützten Vorgangs in Schritt 44 beschrieben. Natürlich ist es auch möglich, daß die Ausführung des geschützten Vorgangs fehlschlägt, weil z.B. die Überprüfung der eingegebenen Geheimzahl keine Übereinstimmung mit dem korrekten Wert ergibt. In diesem Fall wird im vorliegenden Ausführungsbeispiel ebenfalls der in **Fig.** 4 dargestellte Wiederherstellungsvorgang ausgeführt, um die im Sicherungspuffer **30** enthaltenen Einträge **32**, **34** in den nicht-flüchtigen Speicher **22** zu übertragen. In Ausführungsvarianten kann jedoch auch vorgesehen sein, daß der Fehlversuchszähler **26** und die dazugehörigen Fehlererkennungsdaten **28** unmittelbar – ohne Mitwirkung der Transaktionsverwaltung – auf neue Werte gesetzt werden. Es müssen dann lediglich noch – wie in Schritt 46 von **Fig.** 3 – die Einträge **32**, **34** im Sicherungspuffer **30** durch Einschreiben eines Kennzeichenwertes **00** an den Anfang des Sicherungspuffers **30** deaktiviert werden.

Patentansprüche

1. Verfahren zum Verwalten eines Fehlversuchszählers (**26**) in einem nicht-flüchtigen Speicher (**22**) eines tragbaren Datenträgers (**10**), wobei
– der Fehlversuchszähler (**26**) zur Überwachung der Anzahl von Fehlversuchen bei der Ausführung eines geschützten Vorgangs dient, und wobei
– der Datenträger (**10**) einen Sicherungspuffer (**30**) aufweist, in dem Daten speicherbar sind, welche bei einem zumindest im Zusammenhang mit einem Neustart des Datenträgers (**10**) ausgelösten Wiederherstellungsvorgang zumindest in den nicht-flüchtigen Speicher (**22**) des Datenträgers (**10**) einzuschreiben sind, gekennzeichnet durch die Schritte:
– Einschreiben eines Eintrags (**34**) in den Sicherungspuffer (**30**) des Datenträgers (**10**), wobei der Eintrag (**34**) einen Wert enthält, der einem neuen Stand des Fehlversuchszählers (**26**) nach einem angenommenen Fehlversuch entspricht, so daß dieser Wert bei einem Wiederherstellungsvorgang in den Fehlversuchszähler (**26**) eingeschrieben wird, und
– Ausführen (**44**) des geschützten Vorgangs.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der in den Sicherungspuffer (**26**) eingeschriebene Eintrag (**34**) zumindest nach einer erfolgreichen Ausführung des geschützten Vorgangs deaktiviert wird.

3. Verfahren nach Anspruch 1 oder Anspruch 2, dadurch gekennzeichnet, daß nach einem Fehlversuch bei der Ausführung des geschützten Vorgangs der Stand des Fehlversuchszählers (**26**) verändert wird, um den Fehlversuch anzuzeigen, und daß dann der in den Sicherungspuffer (**26**) eingeschriebene Eintrag (**34**) deaktiviert wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß zur Veränderung des Standes des Fehlversuchszählers (**26**) nach einem Fehlversuch und zur Deaktivierung des in den Sicherungspuffer (**26**) eingeschriebenen Eintrags (**34**) der Wiederherstellungsvorgang ausgeführt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß im Zusammenhang einer erfolgreichen Ausführung des geschützten Vorgangs der Stand des Fehlversuchszählers (**26**) unverändert bleibt oder auf einen Initialwert zurückgesetzt wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß der Sicherungspuffer (**30**) Teil eines vom Datenträger (**10**) auch zu anderen Zwecken bereitgestellten Transaktionsmechanismus ist.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß der Eintrag (**34**) im Sicherungspuffer (**30**) als Bestandteil einer Transaktion derart markiert wird, daß die in diesem Eintrag (**34**) enthaltenen Daten bei einem Wiederherstellungsvorgang in den Speicher (**22**) des Datenträgers (**10**) eingeschrieben werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß zumindest der Fehlversuchszähler (**26**) mittels Fehlererkennungsdaten (**28**) auf das Auftreten von Speicherfehlern überwacht wird, und daß in den Sicherungspuffer (**30**) neben dem neuen Stand des Fehlversuchszählers (**26**) auch die dazu gehörigen Fehlererkennungsdaten (**28**) eingeschrieben werden.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß der neue Stand des Fehlversuchszählers (**26**) und die dazu gehörigen Fehlererkennungsdaten (**28**) in umgekehrter Reihenfolge der Verarbeitung bei einem Wiederherstellungsvorgang in den Sicherungspuffer (**30**) geschrieben werden.

10. Verfahren nach Anspruch 8 oder Anspruch 9, dadurch gekennzeichnet, daß auch der Sicherungspuffer (**30**) mittels Fehlererkennungsdaten (EDC) auf das Auftreten von Speicherfehlern überwacht wird.

11. Datenträger (**10**), insbesondere Chipkarte oder Chipmodul, mit einem Prozessorkern (**12**) und einem nicht-flüchtigen Speicher (**22**), wobei der Pro-

zessorkern (**12**) zur Ausführung eines Verfahrens nach einem der Ansprüche 1 bis 10 eingerichtet ist.

12. Computerprogramrnprodukt, das Programmbefehle aufweist, um einen Prozessorkern (**12**) eines tragbaren Datenträgers (**10**) zu veranlassen, ein Verfahren nach einem der Ansprüche 1 bis 10 auszuführen.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

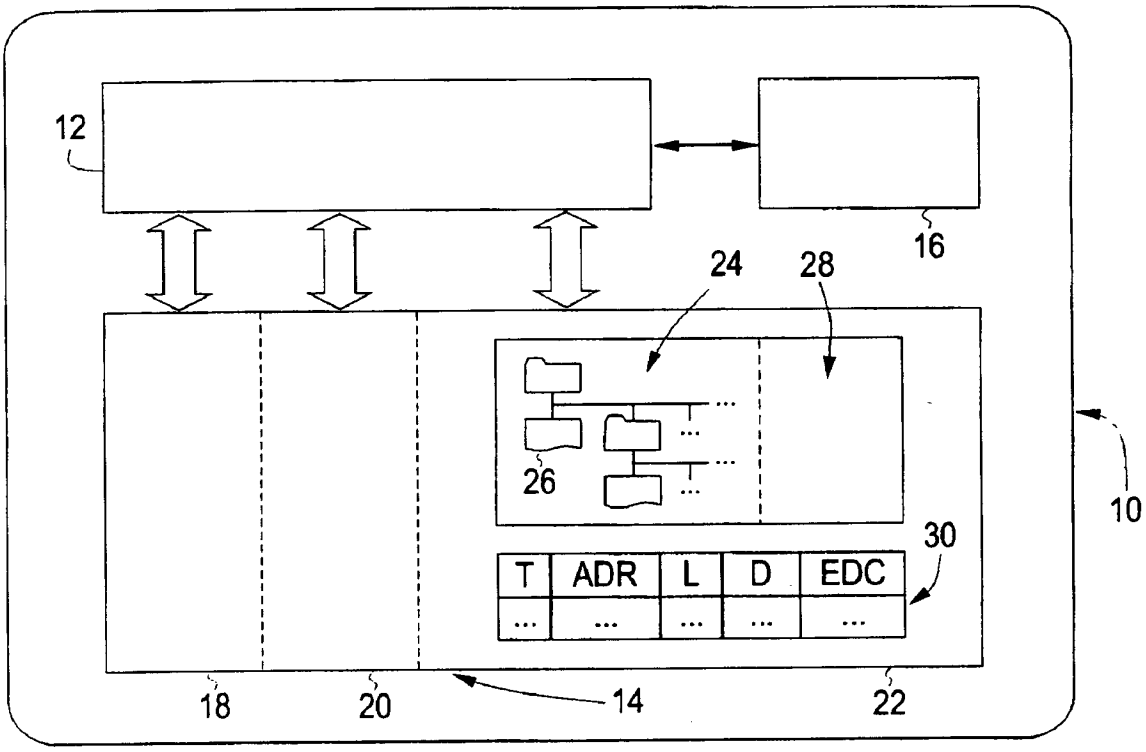


Fig. 1

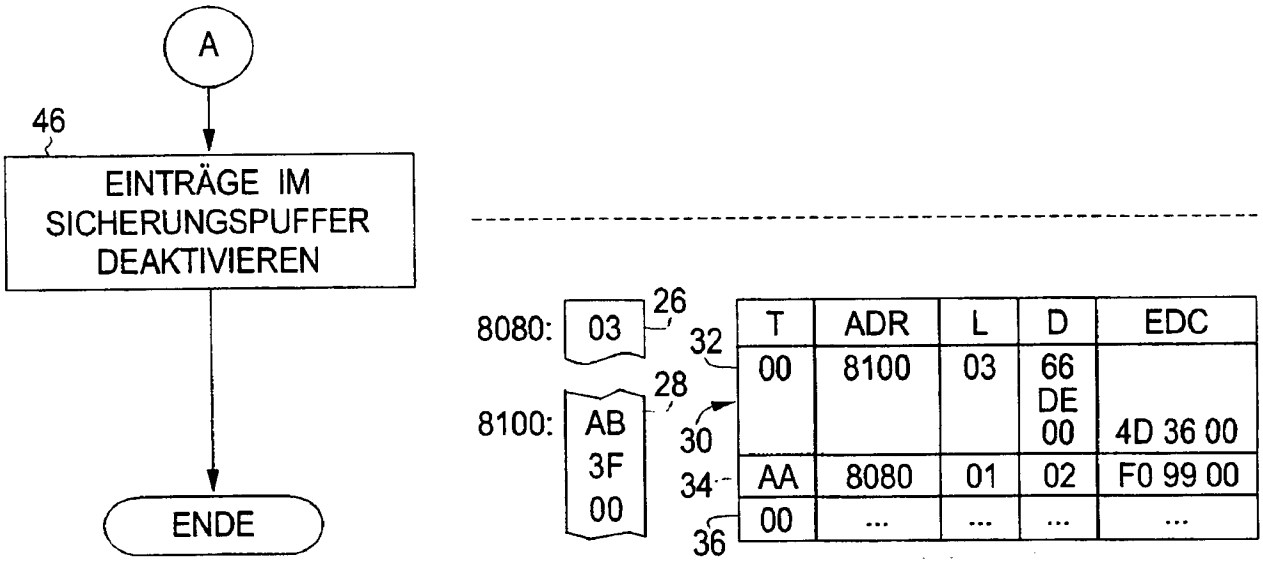


Fig. 3

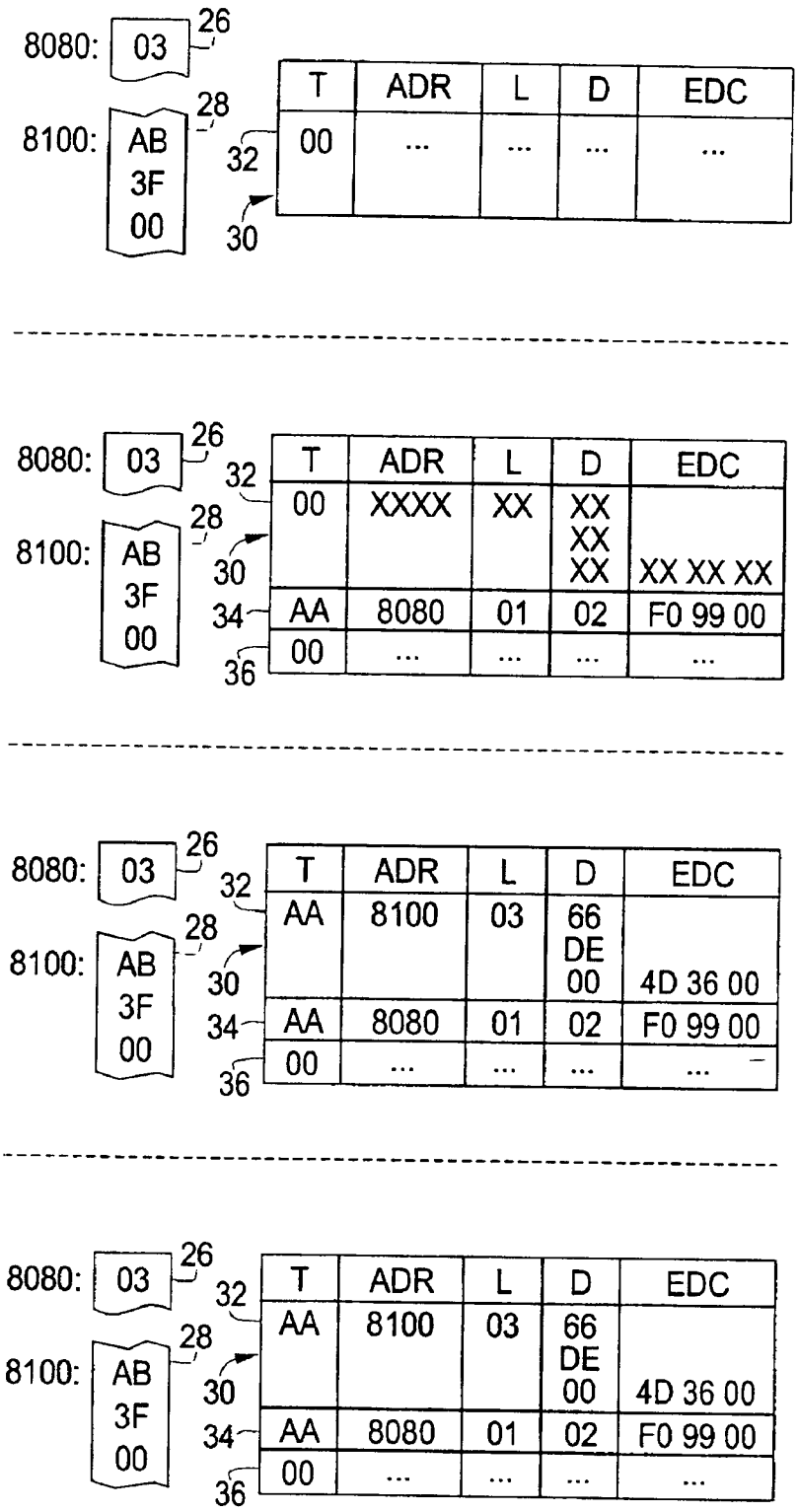


Fig. 2

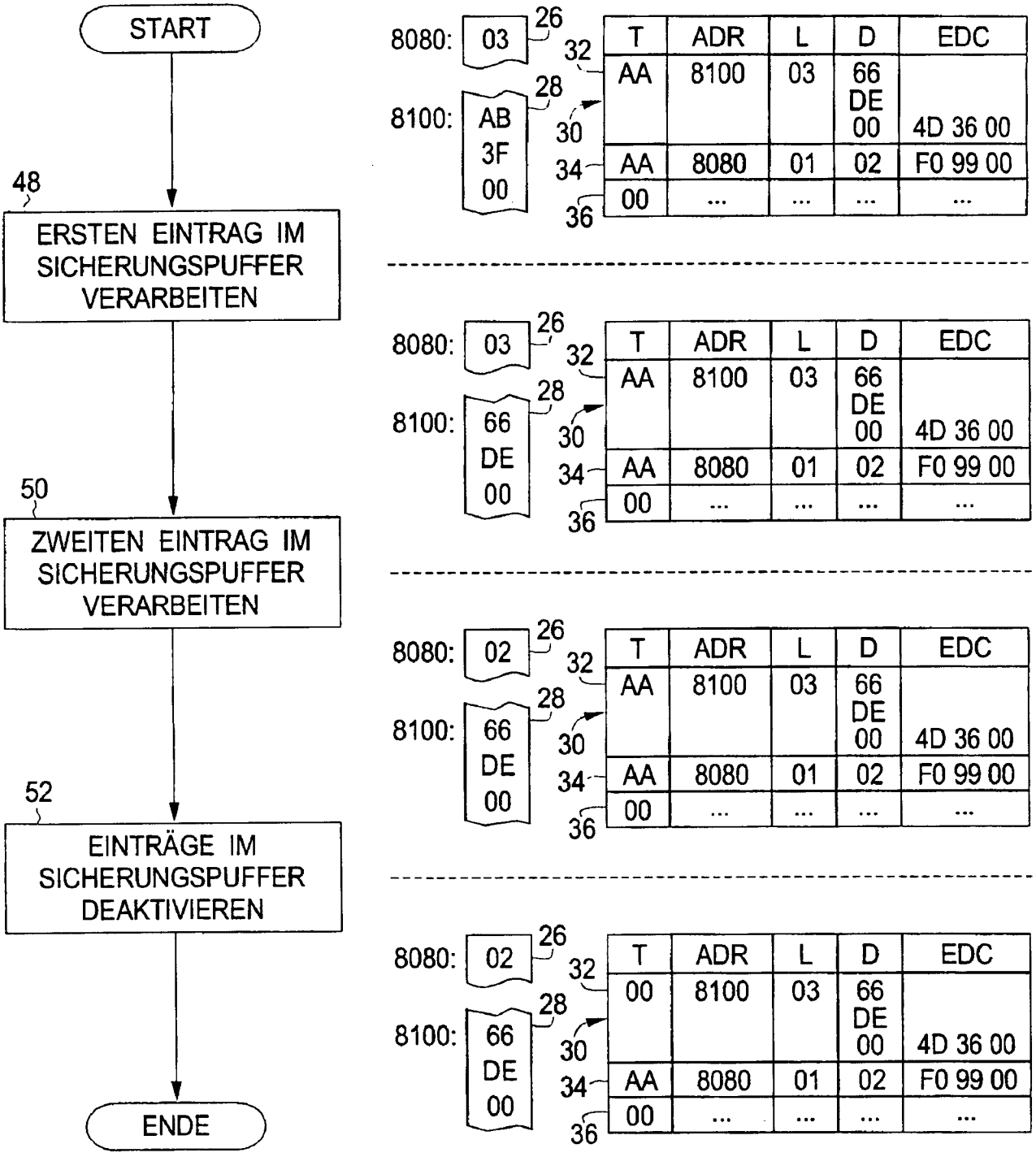


Fig. 4